

ORIGINAL  
CLERK US DISTRICT COURT  
NORTHERN DIST. OF TX  
FILED

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF TEXAS  
DALLAS DIVISION

DEPUTY CLERK

UNITED STATES OF AMERICA

v.

THOMAS JAMES FREDERICK SMITH (1)  
also known as Zook, TJ, and kingsmith007

§  
§  
§  
§  
§  
§

No. 3:09-CR-100-B

FACTUAL RESUME

Defendant Thomas James Frederick Smith, the defendant's attorney Kevin Ross, and the United States of America (the government), agree that the following accurately states the elements of the offense and the facts relevant to the offense to which the defendant is pleading guilty:

Elements:

1. In order for Smith to be convicted at trial of a violation of 18 U.S.C. §371 (18 U.S.C. §§1030(a)(5)(A)(i), 1030(a)(5)(B)(i), and §1030(a)(6)(A)), the United States would have to prove each of the following elements of the offense beyond a reasonable doubt:

- First: Smith and at least one other person made an agreement to commit the crime of [see below violations of 18 U.S.C. §1030] as charged in the indictment;
- Second: Smith knew the unlawful purpose of the agreement and joined in it willfully, that is, with the intent to further the unlawful purpose; and

Third: One of the conspirators during the existence of the conspiracy knowingly committed at least one of the overt acts described in the indictment, in order to accomplish some object or purpose of the conspiracy.

2. The essential elements of a violation of 18 U.S.C. §§1030(a)(5)(A)(i), 1030(a)(5)(B)(i), and §1030(a)(6)(A) are as follows:

First: the defendant knowingly caused the transmission of a program, information, code, or command to a computer;

Second: as a result of the transmission, the defendant intentionally caused damage to a computer without authorization;

Third: the damage resulted in losses to one or more persons totaling at least \$5,000 in value at any time during a one-year period; and

Fourth: the computer damaged was used in interstate or foreign commerce or communication.

3. Smith and codefendant David Anthony Edwards, known to Smith as Davus, agreed and assisted each other to transmit a program, information, code, or command to a protected computer to control the computers, disclose confidential information, or deface a webpage. Specifically, Smith and Edwards knowingly and intentionally did, or assisted each other to:

a. create a coded application file called NETTICK, which could be used to access another person's computer without authorization and gain control over the computer;

b. access other persons' computers without authorization and transmit NETTICK;

c. through the NETTICK, cause the compromised computers (the botnet) to log onto an Internet Relay Chat (IRC) channel hosted on Edward's website kidindustries.net, located on a server in the Northern District of Texas, and wait

for commands;

d. control and command the botnet from the IRC channel hosted on kidindustries.net;

e. cause damage to computers and computer systems.

4. Smith was a member of a hacker forum group called CcpowerForums.com. On or about July 27, 2006, Smith posted a public message on several forums, including CcpowerForums.com, in which he offered to sell or discussed his offer to sell an executable program to control a botnet for \$750; or the source code for \$1,200.

5. On or about October 14, 2006, Smith emailed a potential purchaser, and claimed to possess and control a botnet consisting of 21,892 compromised computers on 3 different servers. Smith offered to sell the botnet for 15 cents each computer, and required a minimum purchase of 5000 compromised computers. Smith also offered to sell the bot source code only if the purchaser bought the entire botnet (all of the compromised computers).

6. On or about August 14, 2006, Smith demonstrated NETTICK's capabilities and caused a portion of the botnet, including one compromised computer in the Northern District of Texas, to engage in a distributed denial of service attack by flooding an IP address at a Internet Service Provider located in the Northern District of Texas.

7. Smith claimed that the demonstration involved only a small portion of his botnet. After the demonstration, the purchaser agreed to buy the source code and the entire botnet for approximately \$3,000, with a \$1,643 downpayment. Smith conducted the

demonstrative DDOS attack through commands given to the compromised computers at irc.Kidindustries.net.

8. On or about August 15, 2006, Smith directed the purchaser to transfer approximately \$1,600 into an E-Gold account number 2880161. Smith caused the down payment to be transferred from the E-Gold account to an IceGold E-Gold account #372. On August 21, 2006, Smith caused a wire transfer from the IceGold E-Gold to Smith's First State Bank checking account xxx898.

9. On or about September 26, 2006, Smith and Edwards accessed without authorization the T35.net user database. T35.net provided free (free-service) and paid personal and business Internet web hosting services for hundreds of thousands of users. The T35.net user database contained confidential user identifications and passwords. Smith and Edwards downloaded the T35.net's user database containing hundreds of thousands of the confidential user identifications and passwords for the free-service clients.

10. On or about October 3, 2006, Smith assisted Edwards in defacing the T35.net website and making the user identifications and passwords of the free-service clients available to the public.

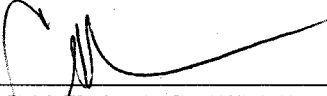
11. On or about October 4, 2006, through an Internet communication, Smith advised T35.net's administrator that the T35.net website had been defaced and its user database compromised. Smith asked the administrator, "How are all the users going to be compensated?"

12. Smith understands that compromising a computer causes damage or a loss to the particular individual whose computer was compromised.

13. Smith understands that T35.net's cost to remediate the compromised database and server exceeded \$5,000.00, but was less than \$10,000.00.

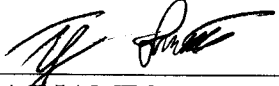
Respectfully Submitted,

JAMES T. JACKS  
UNITED STATES ATTORNEY

  
CANDINA S. HEATH  
Assistant United States Attorney  
Texas State Bar No. 09347450  
1100 Commerce Street, Third Floor  
Dallas, Texas 75242-1699  
Tel: 214.659.8600  
Fax: 214.767.2846  
candina.heath@usdoj.gov

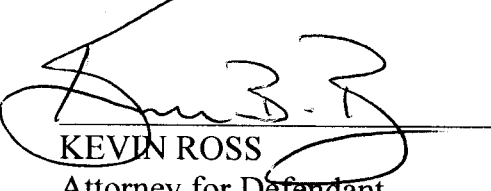
4-14-2010  
Date

I have read (or had read to me) this Factual Resume and have carefully reviewed every part of it with my attorney. I fully understand it and I swear that the facts contained herein are true and correct.

  
THOMAS JAMES FREDERICK SMITH  
Defendant

04/04/28  
Date

I am Thomas James Frederick Smith's counsel. I have carefully reviewed every part of this Factual Resume with my client. To my knowledge and belief, my client's decision execute this Factual Resume is an informed and voluntary one.

  
KEVIN ROSS  
Attorney for Defendant

4/30/2010  
Date